Please Amend the Specification as follows:

Please replace paragraph 0041 on page 4, with the following amended paragraph:

The data integrity of the unencrypted executable is verified at step 506. The secure processor 180 verifies the data integrity of the unencrypted executable by prepending the applet serial number to the unencrypted executable and verifying the executable signature portion 224 using a public key verification algorithm. In a certain embodiment, the Rivest, Shamir and Adleman algorithm is used. Before the applet server 110 downloads the applet, the executable signature portion 224 is created based on the data contained in the unencrypted executable with the applet serial number prepended onto the unencrypted executable. After the executable signature portion 224 is created, the applet serial number is stripped from the unencrypted executable, and the unencrypted executable is encrypted creating the encrypted executable 222. If any information in the encrypted executable 222, the unencrypted executable, or the applet serial number is altered between the time the unencrypted executable signature 216 was created and the time when the verification takes place on the secure processor 180, the verification process will fail. If the verification process fails, the process 300 exits. If the verification process detects no change in the unencrypted executable, the applet 200 can be installed.